

Identity and Security Management Solutions for the SAP® Environment

Table of Contents:	2	Solution Overview
	2	The Role of Identity and Security Management
	3	The Challenges of Identity Management
	4	What Identity and Security Management Can Do for SAP Environments
	6	Extending the Reach of SAP Solutions
	9	Conclusion

Solution Overview

The identity management market is experiencing strong growth fueled by brisk business, personal and public needs for security, regulatory compliance and cost control.

For most organizations, identity and security management—and the associated benefits of tighter security, lower costs and regulatory compliance—requires the integration of user and device identities that are distributed across a wide range of applications, databases and operating systems. The breadth of such integration is a common and worthwhile IT challenge. Automating identity management throughout your enterprise can result in smoother, more secure operations. It can also help you comply with the vast array of regulations your organization faces.

While identity information is included in everything from an e-mail application to corporate white pages, the identity itself often begins in an Enterprise Resource Planning (ERP) application or similar software, such as those offered in the SAP Business Suite. This software addresses functions like human resources (HR) or customer relationship management (CRM). For instance, information about a new employee is typically entered into an HR system before that employee is granted access to any other enterprise applications; a similar starting point is used for customers in a CRM system.

The essential role of these applications in the overall lifecycle of an identity makes them a critical starting point and a key success factor in many identity management deployments. In other words, when an organization decides to manage and monitor identity and access management policy in a coherent, centralized fashion, the first step is to automate user account management and related business processes. This automation begins by making the identities stored in ERP systems available to other enterprise applications.

The Role of Identity and Security Management

The identity management market is experiencing strong growth fueled by brisk business, personal and public needs for security, regulatory compliance and cost control. Governments are increasingly regulating online information—especially information about individuals. Governments worldwide are fueling identity management market activity by issuing regulations for identity information as well as the accountability surrounding its use. Such regulations are forcing organizations to improve their controls over systems and information. As organizations work to upgrade controls over critical infrastructure, identity management is becoming part of that critical infrastructure. Software vendors are therefore rushing to include audit, validation and remediation features in identity management suites.

In addition, historical methods for securing online applications are simply not sustainable from an administrative perspective. The cost of allowing each application to control its own user population and then requiring local administrators to set policies for using application resources is becoming problematic. As users access applications through a variety of mediums—Web browsers, handheld devices and intermediary applications—access and management needs are exceeding the models existing applications were designed to support. Therefore, all enterprise applications require some degree of common security and authorization.

In short, for enterprises, the risks of conducting business online are becoming higher,

but the cost of improving security using current methods is prohibitive. The security costs are also much higher than anticipated because prior funding models viewed security as a control system rather than a business-enabling infrastructure. The focus of identity management vendors, then, is to enable enterprises to increase the security of online systems while reducing administrative costs and improving user satisfaction.

The Challenges of Identity Management

The SAP Business Suite consists of several modules that encompass a wide range of business functions, from human resources and accounting to customer and supply-chain relationship management. In recent versions of the suite, the central point of access for the modules is the SAP NetWeaver® Portal, a Web-based front end for the entire SAP system. Even with a rich portal interface, enterprisewide identity and access management for SAP and other applications presents several challenges. The foremost of these is managing user accounts across SAP modules. This is a time-consuming, expensive and often inaccurate process. In a word, it's manual: it involves entering, modifying or deleting user information—repeatedly—in multiple systems across the enterprise. As the enterprise grows and changes to meet market demands, the challenges of quickly and accurately granting and revoking access rights grows with it. In addition, monitoring processes to ensure compliance to corporate and governmental regulations only add to the burden and costs.

Consider these scenarios:

- *A new employee is added to the SAP ERP Human Capital Management (SAP ERP HCM) application upon joining a company, but overburdened network and application administrators, experiencing time and*

resource constraints, are unable to add that employee to other business systems, including several other SAP modules because it is a manual process.

- *Conversely, a departing employee is removed from SAP ERP HCM, but the need to remove the employee's access to other critical systems is overlooked because of insufficient communications or constrained resources. The lingering account provides a former employee with ongoing access to sensitive information.*
- *An employee's responsibilities within the organization change and because of insufficient monitoring capabilities, a separation of duties situation occurs that violates company and/or governmental regulations.*
- *Following a routine audit, company executives are informed that the lack of consistent access controls and insufficient monitoring for SAP and other critical business systems has left the company in violation of governmental regulations that mandate the protection of sensitive data and financial information.*
- *Because many users are forced to manage an unwieldy number of passwords to access their business systems, the company's IT staff spends more than a third of its time fielding password-related calls, instead of focusing on more strategic projects.*

It is these, and myriad other identity-related challenges, that Novell® addresses with its Identity and Security Management solutions.

For many SAP customers, Identity and Security Management products from Novell deliver the following substantial business benefits:

- **Significantly reduce or eliminate redundant administration costs.**
Because user accounts created, deleted or modified in SAP HCM are automatically

Enterprisewide identity and access management for SAP solutions and other applications presents several challenges. The foremost of these is managing user accounts across various applications. This is a time-consuming, expensive and often inaccurate process. In a word, it's manual.

Corporate security is no longer dependent upon an administrator manually removing a user account from every system.

Identity and Access Management is the set of processes and supporting infrastructure that facilitates the creation, maintenance and use of digital identities across many disparate systems in an enterprise.

propagated across all SAP modules and other enterprise applications, administrators no longer have to waste time and money performing the same task several times. Eliminating that redundant administration not only delivers a reduction in administration costs, but it also allows administrators to focus on more strategic projects.

- **Tighten security.** *When employees' responsibilities change or they leave the organization, it is imperative that their access to corporate resources be modified or deleted appropriately. If access is not updated immediately, separation of duty violations may inadvertently occur or sensitive information may be comprised. This risk is eliminated because you can revoke user access rights across every SAP module and other enterprise applications with a single action. Corporate security is no longer dependent upon an administrator manually removing a user account from every system.*
- **Facilitate organizational changes.** *New employees or employees with shifting responsibilities are more quickly productive because they gain access to the applications they need immediately—instead of waiting days or even weeks.*
- **Simplify password management.** *By reducing the number of passwords users are required to remember, and concurrently enforcing the use of stronger passwords, you can enhance security and make users more productive. In addition, enabling users to reset lost or forgotten passwords themselves allows IT personnel to focus on strategic projects rather than on a consistent stream of mundane password resets.*
- **Ensure enterprise information management.** *Analyzing identity and*

access activities across enterprise systems enables you to automate the data gathering process necessary to prove compliance with corporate and governmental regulations, or to alert application owners or application managers of potential security risks.

What Identity and Security Management Can Do for SAP Environments

Both Identity and Access Management (IAM) and Security Information and Event Management (SIEM) solutions provide operational efficiencies by automating tedious and error-prone manual processes (see Figure 1).

- *Identity and Access Management is the set of processes and supporting infrastructure that facilitates the creation, maintenance and use of digital identities across many disparate systems in an enterprise. Nearly every significant business function—from a simple purchase to demonstrating compliance with government regulations—requires the establishment and use of identity. IAM solutions provide that critical “system of record” for these identities. Account provisioning and single sign-on are other key components of IAM solutions that have contributed to rising interest from mid- to large-sized organizations in recent years.*
- *SIEM solutions continuously collect events and combine the data from these events with in-depth correlation, real-time views and up-to-the-minute reports of activities occurring on multiple enterprise sources. SIEM software provides a “system of record” for remediation processes when security or compliance policies have been violated. SIEM solutions automate collection, analysis, response and reporting activities. As a result, they are valuable additions to IT security programs that need to monitor and protect a broad spectrum of systems and critical assets.*

Figure 1. Integrating solutions provides operational efficiencies

These solutions, while initially coming from different perspectives and serving different target audiences, actually cover two aspects of governance and regulatory compliance. One aspect provides the essential automation controls over identity information. The other provides the necessary validation, ensuring that policies are being followed by all systems under observation. This combination delivers substantial increases in operational efficiency and significantly improves compliance monitoring and reporting.



Combined solutions incorporating Novell Sentinel, Novell Identity Manager and Novell Access Manager give you a real-time, enterprisewide system that can intelligently and automatically respond to any event, whether it's an insider violation by a privileged user or a simple provisioning request.

Novell Delivers a Comprehensive Identity and Security Stack

Novell offers industry-leading identity and security management solutions that facilitate your organization's ability to better control its IT environment. Combined solutions incorporating Novell Sentinel™, Novell Identity Manager and Novell Access Manager™ give you a real-time, enterprisewide system that can intelligently and automatically respond to any event, whether it's an insider violation by a privileged user or a simple provisioning request.

These products work closely with each other and provide coverage across the entire identity management spectrum. Figure 2 on the following page highlights these products relative to the Burton Group's Identity and Privacy Strategies Reference Architecture,

a vendor-neutral perspective on the required components for providing a comprehensive identity management infrastructure. Novell Identity Manager provides a persistent, normalized view of identity. It also gives you the necessary identity provisioning, integration and synchronization between the disparate systems throughout your enterprise, including authoritative sources of identity such as SAP solutions. Novell Access Manager delivers the access policy enforcement infrastructure, including Web access management, authorization and federation services for applications within the enterprise. Novell Sentinel gives you the monitoring, event correlation, policy validation, auditing, and reporting necessary to ensure that the rest of the identity infrastructure is operating in accordance to policy, and that your organization is meeting its compliance objectives.

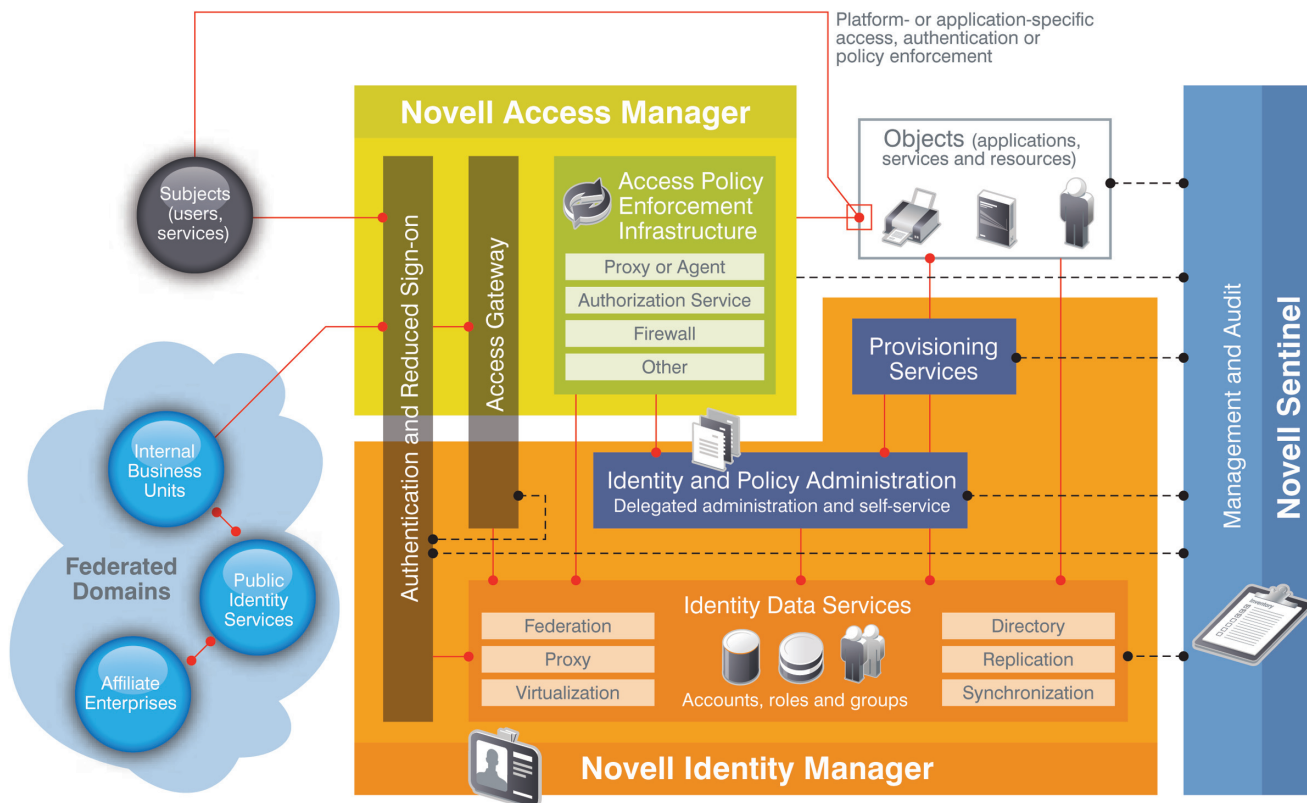


Figure 2. Novell comprehensive identity and security stack

The identity vault in Novell eDirectory (certified for integration with SAP NetWeaver) can incorporate identity aspects throughout SAP NetWeaver integration points. Novell Access Manager can be utilized as an authentication and authorization conduit and extend SAP NetWeaver identity-enabled services to business partners through the use of Liberty-enabled federation capabilities.

Extending the Reach of SAP Solutions

Extending the Reach of SAP NetWeaver

SAP NetWeaver enables application-to-application processes, business-to-business processes, business process management and inserts real-world awareness into businesses processes. SAP NetWeaver delivers a path to an enterprise services architecture blueprint while Novell provides a unique capability to inject identity throughout these processes. The identity vault in Novell eDirectory™ (certified for integration with SAP NetWeaver) can incorporate identity aspects throughout SAP NetWeaver integration points. Novell Access Manager can be utilized as an authentication and authorization conduit and extend SAP NetWeaver identity-enabled services to business partners through the use of Liberty-enabled federation capabilities.

Novell Identity Manager (also certified for integration with SAP NetWeaver) offers a powerful and flexible set of identity synchronization and provisioning capabilities. Leveraging the business roles, processes and policies defined within SAP environments, Novell solutions extend this reach to hundreds of other systems, including:

- Directories
- Databases
- E-mail/collaboration systems
- Helpdesk/ticketing systems
- Physical access control systems
- Telephone systems
- Mainframe systems
- UNIX*/Linux* systems
- Mid-range systems
- RADIUS, 802.1X, VPN and other authentication/access systems

- Routers, switches, firewalls and other network tools
- File systems
- Resource/asset management systems (desktops, handheld devices, servers and so on)
- Systems managed through message queue architecture such as JMS
- And many more

Furthermore, with Web services enabled interfaces, the Novell Identity Manager workflow and approval system can be easily incorporated into the SAP NetWeaver Portal to integrate SAP with other enterprise applications.

Extending the Reach of SAP® BusinessObjects™ for GRC

The functional reach of SAP BusinessObjects for governance, risk and compliance (GRC) extends throughout the SAP application modules. They manage vital provisioning, access control and/or monitoring capabilities. In addition to extending the current capabilities of SAP BusinessObjects for GRC, Novell Sentinel, a leader in the SIEM space, also augments the functionality of SAP BusinessObjects for GRC. Novell is unique among competitors in both the depth and breadth of functionality it delivers and the degree of integration among its components—especially with the industry’s first integration of Identity and Access Management and Security Information and Event Management. This combination enables powerful and flexible policy expression and enforcement capabilities throughout your enterprise applications.

By leveraging the policy definitions within SAP BusinessObjects for GRC, you can take advantage of Novell capabilities, including:

Dynamic Separation of Duties (SoD)

In addition to static SoD, Novell supports session-level SoD. In many businesses, user roles are not inherently mutually exclusive, but an individual user is not allowed to act in certain role combinations simultaneously.

Novell is unique among competitors in both the depth and breadth of functionality it delivers and the degree of integration among its components—especially with the industry’s first integration of Identity and Access Management and Security Information and Event Management.

Once a user logs on to the system, acting in a particular role, Novell solutions prevent the user from acting in conflicting roles during that session. To act in a different, conflicting role, the user must log out of the current session and establish a new session acting in the other role.

Soft Separation of Duties

Similar to dynamic SoD, soft SoD is another way to handle incompatible role combinations. Some duties must be clearly separated at all times (hard SoD). However, experienced audit organizations stress that hard SoD constraints are sometimes overused, leading to an unsustainable conditions for the organization (see Deloitte, *Under Control: Sustaining Compliance with Sarbanes-Oxley in Year Two and Beyond*, 2005).

Many organizations choose to follow a “trust, but verify” philosophy, consistent with the sustainability notion described above. Soft SoD is one control that fits this approach. Under this model, your organization would give users guidance and training on what constitutes inappropriate behavior. In addition to enforcing this approach through strict access prevention, Novell solutions support robust monitoring of all user activity. If a user behaves inappropriately, the Novell solution detects it and can initiate immediate follow-up actions. You can decide the severity of the follow-up action: you can choose an action as gentle as a notification to the user and manager, or perhaps add a more severe

In addition to extending the current capabilities of SAP BusinessObjects for GRC, Novell Sentinel, a leader in the SIEM space, also augments the functionality of SAP BusinessObjects for GRC.

Novell Identity and Security Management solutions readily address the broad range of customers' identity and security requirements. And this fact is supported by thousands of customers worldwide who use these products daily.

Integrating Novell Identity and Security Management solutions with the SAP NetWeaver and GRC offerings extend the reach of SAP solutions to all aspects of the enterprise.

option, such as a temporarily locking the user out from the system in question.

Grace Period Separation of Duties

In a further refinement of the soft SoD concept, the Novell solution supports grace period SoD. This approach not only detects when a user violates appropriate behavior, but also keeps track of the number of occurrences. The organization may then institute an escalating response policy, such as the following:

- *The first time a violation occurs, simply provide notification to user and manager.*
- *The second time, notify the security staff and temporarily lock the user out of the violated system.*
- *The third time, disable all user access to all systems, including physical building access, telephone access and so on, pending a review of the user's activities. Alert the security staff to immediately escort the user off the premises.*

SAP NetWeaver, GRC and Novell

In summary, integrating Novell Identity and Security Management solutions with the SAP NetWeaver and GRC offerings extend the reach of SAP solutions to all aspects of the enterprise. Based on an industry-recognized reference architecture, integrating Identity and Security Management

solutions from Novell will provide SAP customers with:

A Common Architecture—Common Elements Shared between Components:

- *Common event model*
- *Common policy store*
- *Common user store*
- *Common authorization model*
- *Common authentication model*
- *Common administrative tools*
- *Common architecture/modeling tools*
- *Common audit/monitoring architecture*
- *Common cross-platform strategy, including enterprise-class Linux and Linux virtualization*
- *Common language support*
- *Common development process and standards (development tools, testing process and more)*

Inter-product Integration Scenarios:

- *User provisioning that can also provision access policies, physical access, assets, resource management and more*
- *Access management policy decisions that leverage attributes in a common identity store, including federation*
- *Enterprise password management with single sign-on credentials (ESSO and Web SSO) that can be unified with the overall provisioning process*
- *Monitoring is possible for all products, enterprisewide*
- *Monitoring/event correlation which considers events from SAP, the identity suite and all other assets/applications throughout the enterprise*
- *Automated remediation capabilities with enterprise reach*
- *Common audit and compliance reporting that can be incorporated with SAP compliance solutions*

Conclusion

As organizations struggle to deal with increasing IT costs, escalating security risks, and mounting competitive pressure effectively, Novell delivers a positive and optimistic answer to their needs. Novell Identity and Security Management solutions readily address the broad range of customers' identity and security requirements. And this fact is supported by thousands of customers worldwide who use these products daily. Combining the power of SAP BusinessObjects

solutions for GRC and the SAP NetWeaver platform with the strength of Novell Identity and Security Management technologies delivers a comprehensive identity, access and security management solution that effectively removes the barriers that inhibit the flow of security and security information throughout the enterprise. The benefits of such a solution—such as reduced administration costs, accelerated productivity, enhanced security and stronger relationships with employees, customers, partners and suppliers—will be immediate.

Combining the power of the SAP BusinessObjects for GRC framework and the SAP NetWeaver platform with the strength of Novell Identity and Security Management technologies delivers a comprehensive identity, access and security management solution that effectively removes the barriers that inhibit the flow of security and security information throughout the enterprise.

Integrating Novell Identity and Security Management solutions with the SAP NetWeaver and GRC offerings extend the reach of SAP solutions to all aspects of the enterprise. Based on an industry-recognized reference architecture, integrating Identity and Security Management solutions from Novell will provide SAP customers with immediate and tangible benefits.

www.novell.com



Contact your local Novell Solutions Provider, or call Novell at:

1 800 714 3400 U.S./Canada
1 801 861 1349 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.

404 Wyman Street
Waltham, MA 02451 USA